2131 #4
9-3-02

0171.40824X00
NC 28437 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Leon HURST et al
Serial No.:	10/029,349
Filed:	December 28, 2001
For:	IMPROVMENTS IN AND RELATING TO CONSUMPTION OF CONTENT
Group:	2131
Examiner:	To Be Assigned

CLAIM FOR PRIORITY

Assistant Commissioner
of Patents
Washington, D. C. 20231

August 21, 2002

Sir:

Under the provisions of 35 U.S.C. §119 and 37 C.F.R. §l.55, Applicants hereby claim the right of priority based on:

British Patent Appln. No. 0116489.6,
filed July 6, 2001.

A certified copy of the British application is attached.

Respectfully submitted,

Donald E. Stout
Registration No. 26, 422
ANTONELLI, TERRY, STOUT & KRAUS, LLP
(703) 312-6600

Attachment
DES:dlh

INVESTOR IN PEOPLE

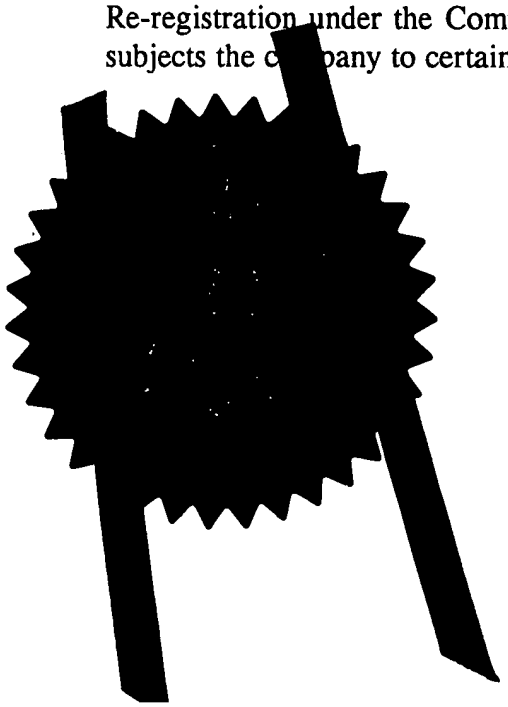
The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



CERTIFIED COPY OF PRIORITY DOCUMENT

Signed A W Brewer.

Dated 10 July 2002

Patents Form 1/77
Patent Acts 1977
(Rule 16)

06JUL01 E643123-1 D02716
P01/7700 0.00-0116489.6

THE PATENT OFFICE
A
-6 JUL 2001
RECEIVED BY FAX

The Patent Office

Request for grant of a patent

1/77

The Patent Office
Cardiff Road
Newport
Gwent NP10 8QQ

1.	Your reference	PAT 01110 GB
2.	Patent application number	0116489.6
		06 JUL 2001
3.	Full name, address and post code of the or of each applicant Patents ADP Number If the applicant is a corporate body, give the country/state of its incorporation	NOKIA CORPORATION Keilalahdentie 4 02150 Espoo Finland 07652217001 Finland
4.	Title of the invention	Improvements in and relating to consumption of content
5.	Name of your agent "Address for service" in the United Kingdom to which all correspondence should be sent Patents ADP number	Nokia IPR Department Nokia House, Summit Avenue Farnborough, Hants GU14 ONG 7577638001 07577638001

6.	If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and the or each application number	Country	Priority Application Number	Date of Filing

7.	If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application	Number of earlier application	Date of Filing

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.

Yes

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	12 ✓
Claims(s)	4 ✓
Abstract	1 ✓
Drawing(s)	7 ✓

10. If you are also filing any of the following state how many against each item.

Priority documents	
Translation of priority documents	
Statement of inventorship and right to grant of a patent (Patents Form 7/77)	
Request for preliminary examination and search (Patents Form 9/77)	1 ✓
Request for substantive examination (Patents Form 10/77)	
Any other documents (please specify)	

11. I/We request the grant of a patent on the basis of this application.

Signature [signature] Date 28/6/01

IAN JOHNSON

12. Name and daytime telephone number of person to contact in the United Kingdom

Ian Johnson 01252 865331

PAT 01110 GB

Improvements in and relating to consumption of content

The present invention relates to the consumption of content, particularly although not exclusively the distribution, rendering and decryption of content having digital rights such as copyright therein.

Typically, content such as video, audio or textual data is consumed by a user via a terminal such as a rendering machine. A rendering machine transforms the data defining the content into a form which may be interpreted by a user's senses. Thus, content in the form of video may be rendered on a visual display unit or monitor, audio content may be rendered by a stereo system and a printer used to render textual content, to name but a few examples. In many cases, such as the distribution of content recorded on magnetic media, optical disk or the like, a number of stages will take place in rendering the data to a form suitable for interpretation by a user's senses.

With the advent of digital content distribution, the opportunity has arisen for faultless replication of content to be carried out. Clearly, without appropriate controls, such replication or copying can take place without the agreement of a relevant right holder. A particular challenge to the content generating community, which includes record companies, publishers and other right holders, is the ease with which digital content may be disseminated, particularly over networks. This ease of dissemination is also coupled with the fact that there is little or no degradation in the quality of the content despite repeat copying and forwarding of the content in its original format. Thus, unauthorised copies of copyright context will meet the same high expectations of consumers in relation to the authorised content.

Consequently, many approaches have been implemented and are being developed to protecting such content for rendering on a particular rendering machine. A particularly favoured approach (Figure 3) is to provide each

rendering machine 2 with a globally unique tamperproof identity 4 and to incorporate a Digital Rights Management engine 6 into the device 2. Subsequently, content stored in encrypted form on the device 2 may be unlocked only where licence conditions, including a requirement to confirm that the globally unique identity 4 of the device 2 matches a set of binding attributes in the licence, are met.

According to one aspect of the present invention, there is provided a method of decrypting content stored on a terminal, the method comprising obtaining a licence containing a content decryption key and a set of binding attributes including a public key, establishing a channel to at least one other terminal and receiving, in response to a request made over said channel, digitally signed data, verifying said digitally signed data utilising said public key wherein decryption of said content using said content decryption key is conditional upon successful verification.

By binding content to a consumer identity, preferably in the form of an asymmetric key-pair the private key being held in a Personal Trusted Device (PTD) of the user, the content is no longer bound to a particular terminal such as a rendering machine. As a result, the consumer is able to enjoy content in any suitable rendering machine wherever she is able to prove her identity through the presence of her personal trusted device or more particularly through the presence of her private key on a secure tamperproof security element accessible to a protected processing environment (PPE) of her personal trusted device. Such a PPE provides functions including the ability to digitally sign data e.g. text, for the purposes of authentication, for example. The choice of whether symmetric or asymmetric encryption techniques are utilised to protect the content, any associated business rules or other conditions relating to the content, may depend not only on the preferences of the right holder, but also on technical considerations relating to security, ease and/or speed of encryption/decryption, key distribution and the like. Indeed, a hybrid approach may be taken in which both asymmetric and symmetric

encryption schemes are adopted to encrypt content, business rules and other conditions relevant thereto.

According to a further aspect of the present invention, there is provided a terminal for rendering encrypted content, the terminal comprising storage for said encrypted content and a licence containing a content decryption key and a set of binding attributes including a public key, the terminal further comprising a personal area network interface operable to establish a channel to at least one other terminal and to deliver digitally signed data received from said other terminal to a protected processing environment wherein said environment is operable to decrypt said encrypted content using said content decryption key following successful verification of said digitally signed data using said public key.

Conveniently, the protected processing environment includes a digital rights management engine operable in accordance with said binding attributes.

According to a still further aspect of the present invention, there is provided a licence creation method for facilitating the decryption of content on a terminal, the method comprising appending a set of binding attributes to a content decryption key wherein the binding attributes include a public key certificate obtained from a repository holding a public key certificate of a licensee, the corresponding private key being held on another terminal.

The licence creation method is most conveniently under the control of the content provider or a party authorised thereby. Thus, the content provider should be able to verify the identity of those customers to whom it provides access to encrypted content in the form of a licence. Such verification of identity may be carried out by authenticating those certificates obtained from the repository with the relevant certification authority. Clearly, the content provider is able to assess a level of trust in each customer based on the results of verification and the nature of the certification authority. This level of

trust may be utilised by the content provider in determining what rights, if any, should be given in the licence. Such rights may conveniently be stored in a voucher attached to the licence or alternatively the content. Whether the voucher is attached or otherwise delivered with the content or licence, the DRM engine of a terminal should be able to parse the voucher and act in accordance with any restrictions set by the content provider in terms of the granted rights. It will be further apparent that the licence may include a plurality of binding attributes which may allow content to be rendered by corresponding user identities. In which case, the content provider may establish different conditions to the rendering of the content as parsed from a corresponding voucher by a DRM engine of a terminal. Although the licence may only be delivered to a user on payment of a fee for example, advantageously it may only be utilised to access content provided the relevant binding attributes can be satisfied, namely through the above described mechanism. Consequently, the licence is freely transferable over a network or indeed any insecure channel.

According to a yet further aspect of the invention, there is provided a method of distributing encrypted content to a terminal comprising delivering encrypted content and a licence relating thereto to a terminal, said licence containing binding attributes corresponding to a user identity, and requesting authentication of said attributes by a personal trusted device.

It will be apparent that the personal trusted device may be utilised to authenticate the attributes of a licence irrespective of the particular platform on which the content is to be rendered, provided the requisite communication can be established.

In order to understand more fully the present invention a particular embodiment thereof will now be described by way of example and with reference to the accompanying drawings, in which:

Figure 1 is a diagrammatic representation of encrypted content and an associated voucher helpful for use in understanding the present invention;

Figure 2 is a diagrammatic representation of an encrypted licence in accordance with one aspect of the present invention;

Figure 3 is a schematic view of a prior art content rendering system;

Figure 4 is a schematic view of a content rendering system according to a further aspect of the present invention;

Figure 5 is a diagrammatic view of personal trusted device of the system of the system of Figure 4;

Figure 6 is a diagrammatic view of a rendering machine of the system of figure 4;

Figure 7 is a schematic view of the system of Figure 4;

Figure 8a to 8d are example screen displays of the rendering machine of Figure 6; and

Figure 9 is a flow chart illustrating a method according to a still further aspect of the present invention.

Referring to Figure 1, content 1 for delivery to a terminal, hereinafter referred to as a rendering machine is, in this case, packaged together with a voucher 3 defining a set of conditions applying to the rendering of that content 1. By way of example, the conditions may describe the technical requirements for rendering the content 1 and/or additional metadata such as copyright and distribution rights information. The entire package of content and metadata is protected against unauthorised access by symmetric encryption 5. Typically, the strength of the symmetric encryption technology is at least 128bits and a suitable symmetric encryption algorithm might be that set out in the Advanced Encryption Standard (AES) draft proposal for a Federal Information Processing Standard (FIPS) dated 28 February 2001.

In addition to packaging the content 1 securely, the content owner or a party authorised thereby, generates a licence 7 pertaining to that content. Referring to Figure 2 in particular, the licence 7 comprises encrypted 9 and unencrypted

11 portions. The unencrypted portion 11 incorporates metadata identifying the content 1 to which it relates. Because this metadata is unencrypted it is visible to external services required to manipulate the licence and its corresponding content such as those services provided by a Digital Rights Management (DRM) engine and exemplified by certain security aspects of the Wireless Application Protocol Identity Module specification (WIM) published by the Wireless Application Forum, Limited and dated 18 February 2000. The encrypted portion 9 of the licence 7 contains a symmetric content key 13 and a set of binding attributes 15. The key 13 enables access to the corresponding content 1 whilst the binding attributes 15 relate to user identification data which will be elaborated upon below. Similarly, the encrypted portion 9 of the licence 7 is manipulated by those external services required to manipulate the licence 7 and its corresponding content 1 such as those services provided by the Digital Rights Management (DRM) engine and exemplified by certain further security aspects of the Wireless Application Protocol Identity Module specification (WIM) published by the Wireless Application Forum, Limited and dated 18 February 2000. The encryption used to protect the above-described encrypted portion 9 of the licence 7 utilises asymmetric encryption techniques.

Referring generally to Figure 7, a public key 17 of an asymmetric key pair is utilised to encrypt the encrypted portion 9. The public key 17 forms part of a key pair the other half of which, namely the private key 91, is required to decrypt (**A**) the protected portion 9 and thus obtain access to the symmetric content key 13 required to unlock (**C**) the content 1. The key pair comprising the public key 17 and private key 91 protecting the encrypted licence portion is generated by or on behalf of a content provider and remains under the content provider's control. In particular, the content provider is able to control to whom the licence 7 is delivered. Typically, delivery of the licence 7 will be contingent on payment of an appropriate fee or the like.

With reference to Figure 4, there is shown a plurality of content rendering machines 19a, 19b, 19c and a number of Personal Trusted Devices (PTD) 21a, 21b, 21c. The plurality of content rendering machines 19a, 19b, 19c includes both portable and fixed equipment. In addition, the rendering machines 19a, 19b, 19c need not be in the same ownership as a PTD 21a 21b, 21c or any of them.

Each PTD 21a, 21b, 21c has a networking capability with which it can communicate with a rendering machine. Typically, such a capability is provided by a Personal Area Network (PAN) through the provision of one or more technologies from the following non-exhaustive list, namely wireless connectivity such as Infra Red, Low Power Radio Frequency and wired connectivity such as parallel, serial, USB, IEEE 1394 and the like. The extent of each PAN is shown by respective chain lines 23a, 23b, 23c. The PAN may overlap as shown. The PAN capability is interfaced with the known functionality of a mobile terminal as is well known to those skilled in the art.

Referring to Figure 5, thus each PTD 21a, 21b, 23c includes a display 29, a data entry device such as a keypad 31, a transceiver 33 and antenna 35, a general memory 37, a controller 39 and the aforementioned connectivity provided by a wireless interface 25 and wired interface 27. In addition, the PTD 21 is provided with audio/video outputs 41 as well as a headphone jack 43, a speaker 45 and a microphone 47. The general memory 37 which includes Read Only and Random Access portions (ROM, RAM) 49, 51 provides storage for the code necessary to implement the PTD 21 functions and also storage for data which has been generated, received or otherwise utilised by the PTD 21 except to the extent that the function is carried out by or relates to a Protected Processing Environment (PPE) 53. The operation of the mobile telephone functions of the PTD in relation to a wireless network is, of course, well understood by those skilled in the art.

In addition to the known functionality of a mobile terminal, the PTD 21 also includes a Protected Processing Environment (PPE) 53. The PPE 53 of the PTD 21 implements the functionality required to provide authentication through a set of services including providing digital signatures and as exemplified by the Wireless Application Protocol Identity Module specification (WIM) published by the Wireless Application Forum, Limited and dated 18 February 2000. In addition to the connection to the controller 39, the PPE 53 is connected to a Security Element Interface 55 providing a secure access channel to a tamper resistant storage module, hereinafter referred to as a Security Element (SE) 57. The SE 57 holds private keys, certificates and other personal data belonging to a user. The SE 57 inhibits access to the data stored therein by a combination of physical and software barriers the principles of which will be well known to those skilled in the art. The SE or vault 57 facilitates the storage of a private key 59 forming part of an asymmetric key pair owned by the SE 57 owner which in the event the SE 57 is not a permanent component of the terminal 21 will most probably, but not necessarily, correspond to the owner of the terminal 21 in which the SE 57 is installed. Referring to Figure 7, the corresponding public key 93 is made available to third parties as a constituent of a certificate 61 issued and digitally signed by a certification authority (CA). For convenience of access, the certificate 61 is stored on a repository (not shown) to which a content provider, amongst others has read privileges.

Turning now to the rendering machines 19a, 19b, 19c of Figure 4, each has a general architecture shown in Figure 6. Each rendering machine 19, therefore comprises hardware including a controller 73 and a PAN interface utilising one or more connectivity options including wireless connectivity 63 such as IR and LPRF and wired connectivity 65 such serial, parallel, USB, IEEE 1394 and the like. In addition to the function set out below, the PAN interfaces permit the delivery of encrypted content and/or licences to the rendering machine 19. For example, a USB cable 71 may be attached between a portable rendering machine 19a and a Personal Computer (PC) 67

having a connection to the Internet 69 or an internal CD drive. Encrypted content such as music could then be delivered over the cable 71 and stored in the rendering machine 19a for later enjoyment provided the necessary licence conditions were met for rendering the content.

Where the rendering machine 19 relies on addition external components to deliver rendered content to a user, then a suitable output 75 is provided for delivering rendered content to a monitor, audio amplifier or the like 77. Alternatively, the rendered content is output through a display 79 and loudspeaker 81. In addition to the connectivity 63, 65, the device 19 further includes storage means in the form of memory 81 provided to accommodate the large volume of data necessary to store encrypted content in the form of video and audio data files, for example. The rendering machine 19 further incorporates a Digital Rights Management (DRM) engine 83 which is connected to a Security Element (SE) 85 via a security element interface 87. Referring additionally to Figure 7, the SE 85 has provision for storing at least one licence private key 91 necessary to decrypt the licence 7, a portion of which is encrypted using the corresponding public key 17 of the licence public-private key. As will be described further below, the DRM engine 83provides the necessary functionality to administer the usage of content based on the aforementioned licences distributed by the content provider. Such functionality includes the ability, expanded upon below, by which an identity of a user is verified.

Referring again also to Figure 7, the rendering machine 19 SE 85 has the licence key 91 of a content provider already installed thereon which may be used subsequently to decrypt (A) licences 7 delivered to the rendering machine 19, these licences being encrypted with the corresponding public key of the content provider. In due course, a user of the rendering machine 19 may choose to have encrypted content 1 delivered to the device 19 which encrypted content 1 is then held in memory 81. In order to decrypt the

content 1 and subsequently render it to the user it is necessary to obtain an appropriate licence 7 from the content provider. Such a licence 7 may be delivered with the content 1 or could be obtained separately over a different channel and/or at different time.

As has been mentioned above, the licence 7 contains a set of binding attributes 15. These attributes 15 are required to ensure that only a party authorised by the content provider namely the licensor is capable of extracting the symmetrical key 13 required to decrypt the encrypted content 1 from the licence. Typically, delivery of the licences 7 by the licensor takes place after consideration of some form has been provided by the licensee. Such consideration could be monetary or it could relate to a commitment to maintain confidentiality in respect of the content. The particular nature of the consideration, if any, will depend on the particular circumstances.

The binding attributes 15 are provided in the form of a Public Key Infrastructure (PKI) user certificate 61 which is representative of the licensee identity. The certificate 61 contains a public key 93 of the licensee which is preferably digitally signed by a Certification Authority (CA). In an initial step of the licensing process, the licensor may assess to what extent it trusts the certificate of a potential licensee and this may include a determination of the level of trust in the CA and, of course, whether the certificate has been appropriately signed.

With additional reference to Figure 8a to 8d in particular, the user of the rendering machine 19 first selects which encrypted content she desires to render. Thus, via the UI, a list of encrypted content is displayed on the display (Figure 8a). The user selects an encrypted content item from the list and the UI passes an instruction to the controller 73 which in turn is passed to the DRM engine 83. The DRM engine 83 of the rendering machine 19 first searches for a licence 7 corresponding to the content for which a request to render has been received by the UI. Thus, the DRM engine 83 attempts to

match the identity of the encrypted content 1 with the identity data in the exposed portion 11 of any licence stored on the device 19. In the event, no licence can be found, the DRM engine 83 indicates as such to the controller which causes the UI to display an error message on the display (Figure 8b). Otherwise, the DRM engine 83 utilises the licence private key 91 to unlock (**A**) the encryption surrounding the content key 13 and binding attributes 15. However, before the content key 13 is extracted for decryption purposes (**C**), the DRM engine 83 firstly accesses the binding attributes 15, namely the user certificate 61. As has been stated, this certificate 61 contains a public key 93 of a user to whom a licence has been given to render the content 1. The DRM engine 83 instructs the controller 73 to commence polling local PTDs 21 forming a PAN 23 in which the rendering machine 19 is a member. The polling request (**B**) further contains the instruction to the PTDs 21 within the PAN to digitally sign a randomly generated text with a private key 59 stored in the PTDs SE 57 and to return (**B'**) the randomly generated text and corresponding signature as a response to the poll to the rendering machine 19. Figure 9 illustrates the above process in more detail. A hashing algorithm 97 generates a one-way hash 99 of a particular piece of randomly generated data 101 and then encrypts 103 the hash 99 utilising the user private key 59 stored in the SE 57 to form a digital signature 105. The signature 105 and corresponding randomly generated text 101 is received via each device within the PAN 23 and the DRM engine of the rendering machine 19. Thus, the DRM engine 83 takes the randomly generated text 101 returned from each device 21 and subjects it to the same hashing algorithm 97 to form a one way hash 99. This hash 99 is compared 109 with the results of the decryption 107 of the corresponding signature 105 carried out utilising the public key 93 stored in the certificate 61 forming the binding attributes 15 namely a further one way hash 111. In the event that the hashes 99, 111 are not identical then this is an indication that the public key of the certificate is not the pair of the user private key on that PTD 21. Thus, the DRM engine 83 does not permit the extraction of the symmetric key 13 necessary to decrypt the encrypted

content 1. Subsequently, where no other PTD 21 has responded to the poll then the DRM engine 83 instructs the controller 73 to indicate via the UI that the content cannot be accessed. Thus, a message to this effect is delivered on the display via the UI (Figure 8c). However, where further devices 29 have responded to the poll, the process of creating a one way hash 99 of the received random data 101 and comparing it with the one-way hash 111 derived by decrypting 107 the digital signature 105 using the certificate public key 93 is repeated. In the event that the decrypted one way hash 111 corresponds to the one way hash 99 formed from the random data 101 then the DRM engine 83 is assured that the PTD 21 is established as being in the possession of the user identity licensed to render the content 1. Consequently, the DRM engine 83 permits the content key 13 to be extracted and used to decrypt the content 1. This includes decrypting the business rules 3 associated with the content 1 which may further determine what actions may be carried out in relation to the content 1 by the user. The successful decryption and any associated rules relating to use of the content are delivered to the display of the rendering machine (Figure 8d).

It will be appreciated by those skilled in the art that the functionality of the rendering machine set out above may be provided through software, hardware or any combination thereof.

Claims:

1. A method of decrypting content stored on a terminal, the method comprising obtaining a licence containing a content decryption key and a set of binding attributes including a public key, establishing a channel to at least one other terminal and receiving, in response to a request made over said channel, digitally signed data, verifying said digitally signed data utilising said public key, wherein decryption of said content using said content decryption key is conditional upon successful verification.

2. A method as claimed in Claim 1, including further encrypting at least said content decryption key.

3. A method as claimed in Claim 2, wherein said further encryption is performed using a public key of an asymmetric key pair such that decryption of said content decryption key is carried out using a private key of said asymmetric key pair.

4. A method as claimed in Claim 3, wherein the private key is stored in a tamperproof and secure location.

5. A method as claimed in Claim 4, wherein the secure location comprises a security element.

6. A computer program comprising executable code for execution when loaded on a computer, wherein the computer is operable in accordance with said code to carry out the method according to any one of Claims 1 to 5.

7. A program as claimed in Claim 6, stored in a computer readable medium.

8. A terminal for rendering encrypted content, the terminal comprising storage for said encrypted content and a licence containing a content decryption key and a set of binding attributes including a public key, the terminal further comprising a personal area network interface operable to establish a channel to at least one other terminal and to deliver digitally signed data received from said other terminal to a protected processing environment wherein said environment is operable to decrypt said encrypted content using said content decryption key following successful verification of said digitally signed data using said public key.

9. A terminal as claimed in Claim 8, including tamperproof and secure storage for a private key of an asymmetric key pair wherein said protected processing environment is operable to decrypt at least said content decryption key, said content decryption key having been encrypted using a public key of said asymmetric key pair.

10. A terminal as claimed in Claim 9, wherein said storage is provided by a security element.

11. A terminal as claimed in any one of Claims 8 to 10, wherein said digitally signed data is delivered to said storage.

12. A terminal as claimed in any one of Claims 8 to 11, wherein said protected processing environment is operable to verify said digitally signed data.

13. A terminal as claimed in any one of Claims 8 to 12, wherein said personal area network interface is operable to issue a request to said other terminal to provide digitally signed data.

14. A licence creation method for facilitating the decryption of content on a terminal, the method comprising appending a set of binding attributes to a content decryption key wherein the binding attributes include a public key certificate obtained from a repository holding a public key certificate of a licensee, a corresponding private key being held on another terminal.

15. A method as claimed in Claim 14, including further encrypting at least said content decryption key.

16. A method as claimed in Claim 15, including distributing to said terminal a decryption key for decrypting said encrypted content key.

17. A method as claimed in any one of Claims 14 to 16, wherein a plurality of binding attributes each having a respective public key certificate of a licensee are appended to said content decryption key.

18. A computer program comprising executable code for execution when loaded on a computer, wherein the computer is operable in accordance with said code to carry out the method according to any one of Claims 14 to 17.

19. A program as claimed in Claim 18, stored in a computer readable medium.

20. A method of distributing encrypted content to a rendering machine comprising delivering encrypted content and a licence relating thereto to a rendering machine, said licence containing binding attributes corresponding to a user identity, and requesting authentication of said attributes by a personal trusted device.

21. A method as claimed in Claim 20, including storing a licence decryption key on said rendering machine.

22. A method as claimed in Claim 21, wherein said licence decryption key is a private key such that a corresponding public key is used to encrypt said licence.

23. A method as claimed in any one of Claims 20 to 22, wherein the binding attributes comprise a public key certificate of a user.

24. A method as claimed in Claim 23, wherein the authentication of said attributes comprises a request to provide digitally signed data.

25. A computer program comprising executable code for execution when loaded on a computer, wherein the computer is operable in accordance with said code to carry out the method according to any one of Claims 20 to 24.

26. A program as claimed in Claim 25, stored in a computer readable medium.

Abstract

Improvements in and relating to consumption of content

A method and apparatus for consumption of content (1) is described in which a licensor is able to exercise control over consumption based on a personal identity in the form of a set of binding attributes (15). The control may be exercised for a number of consuming terminals (19) including rendering machines such as portable video and audio players.

Fig. 4

This Page Blank (uspto)

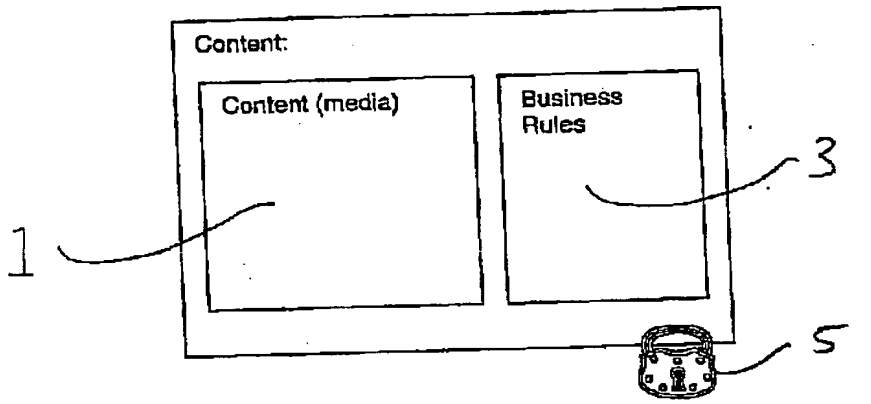


Figure 1

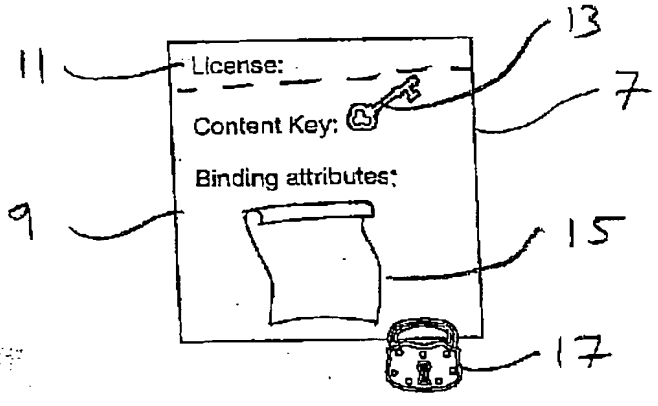


Figure 2

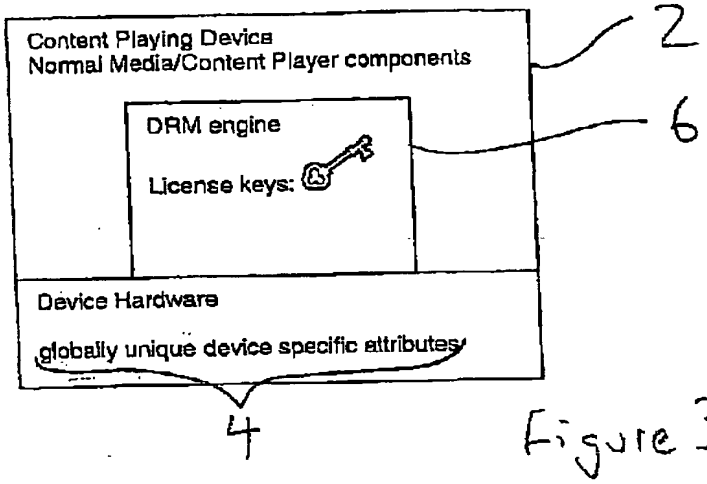


Figure 3

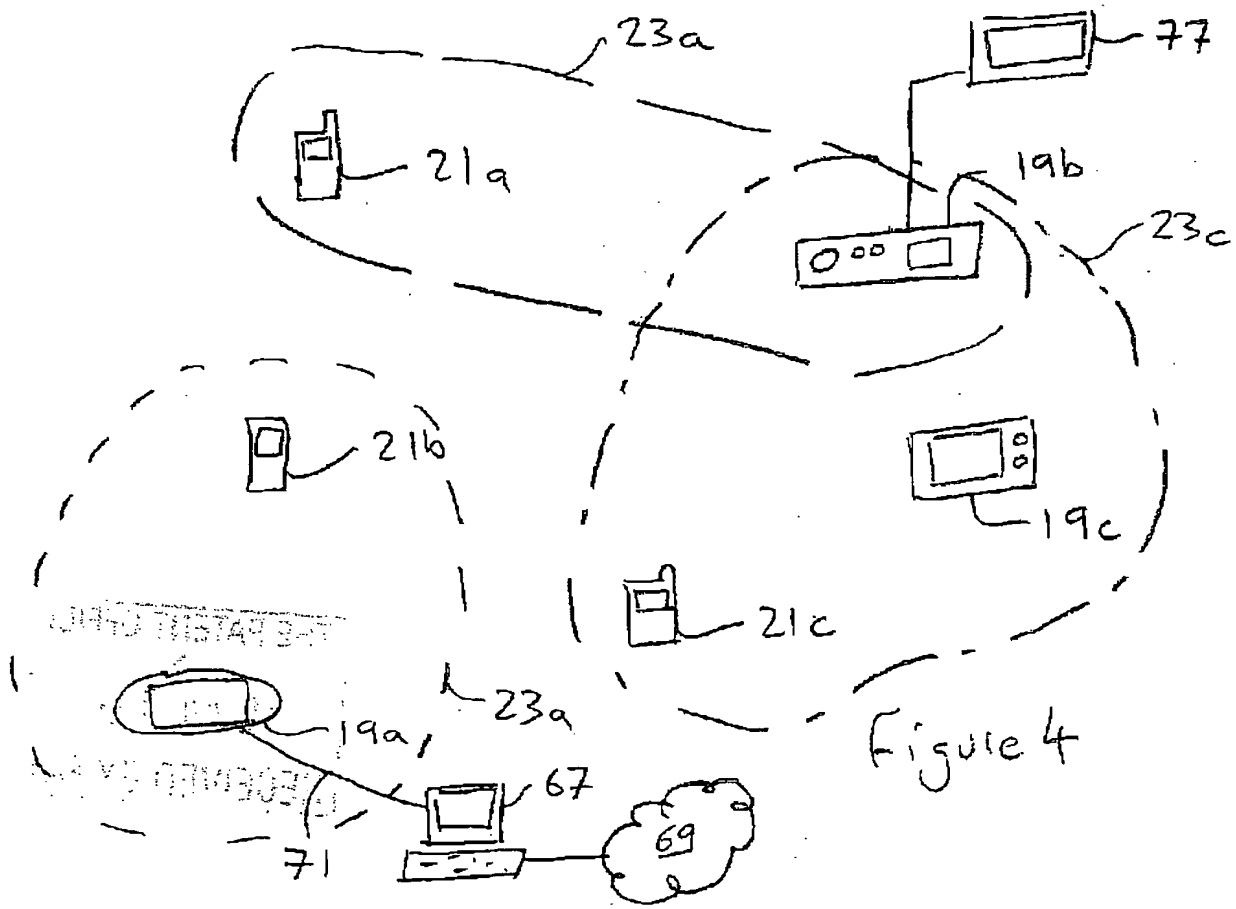


Figure 4

This Page Blank (uspto)

317

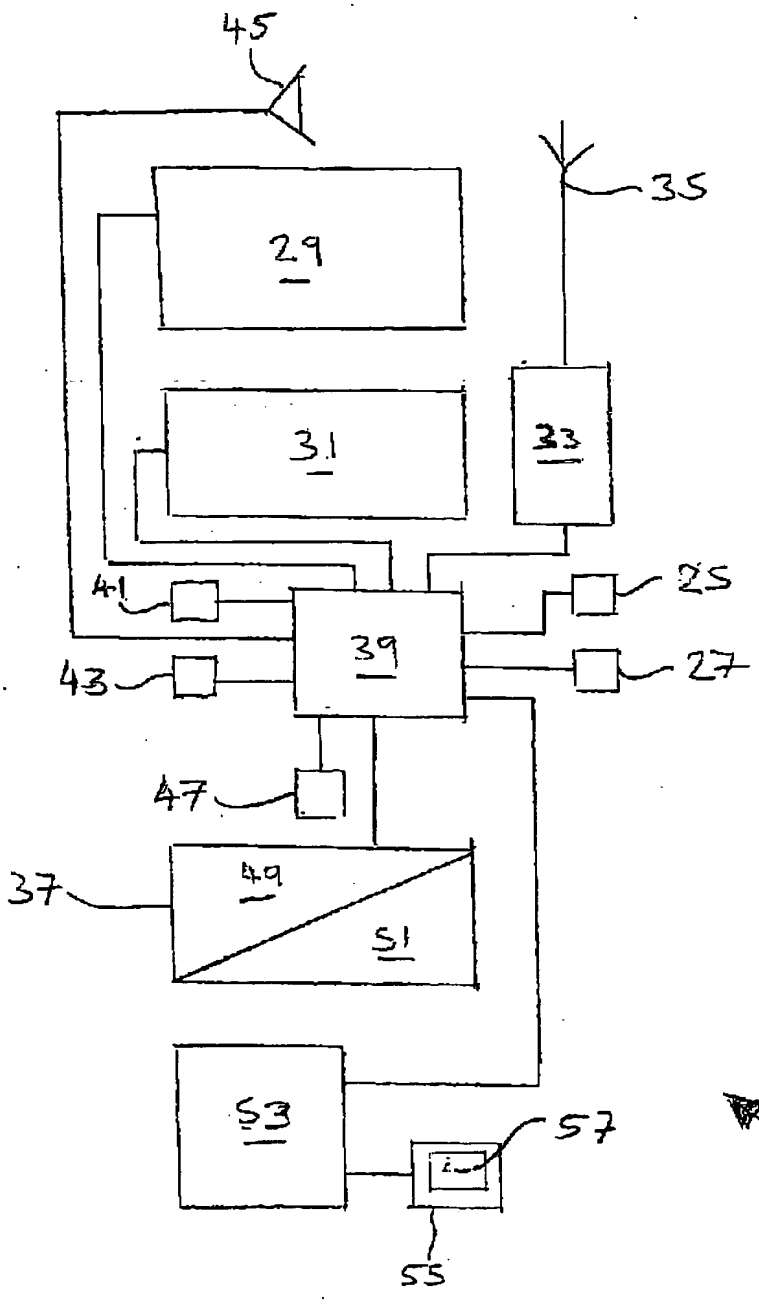


Figure 5

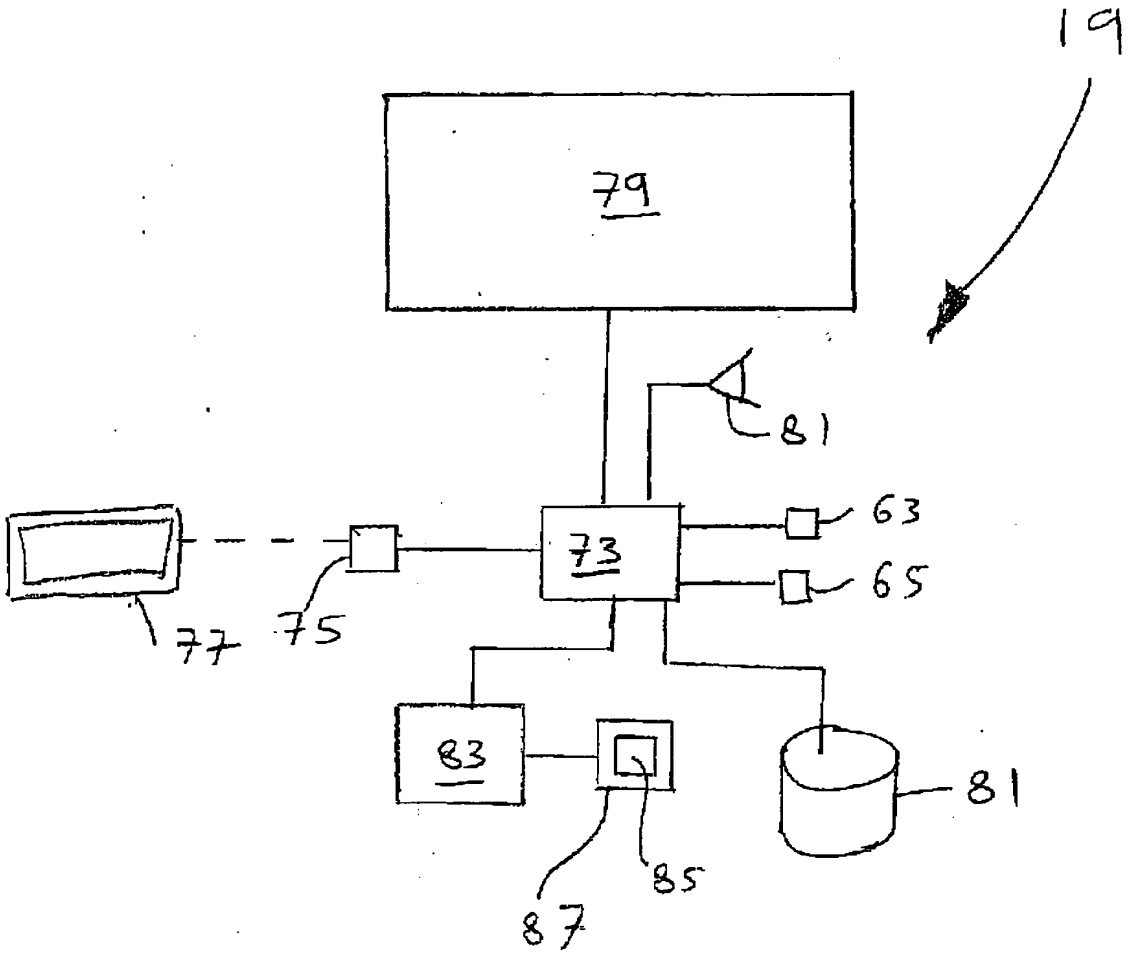


Figure 6

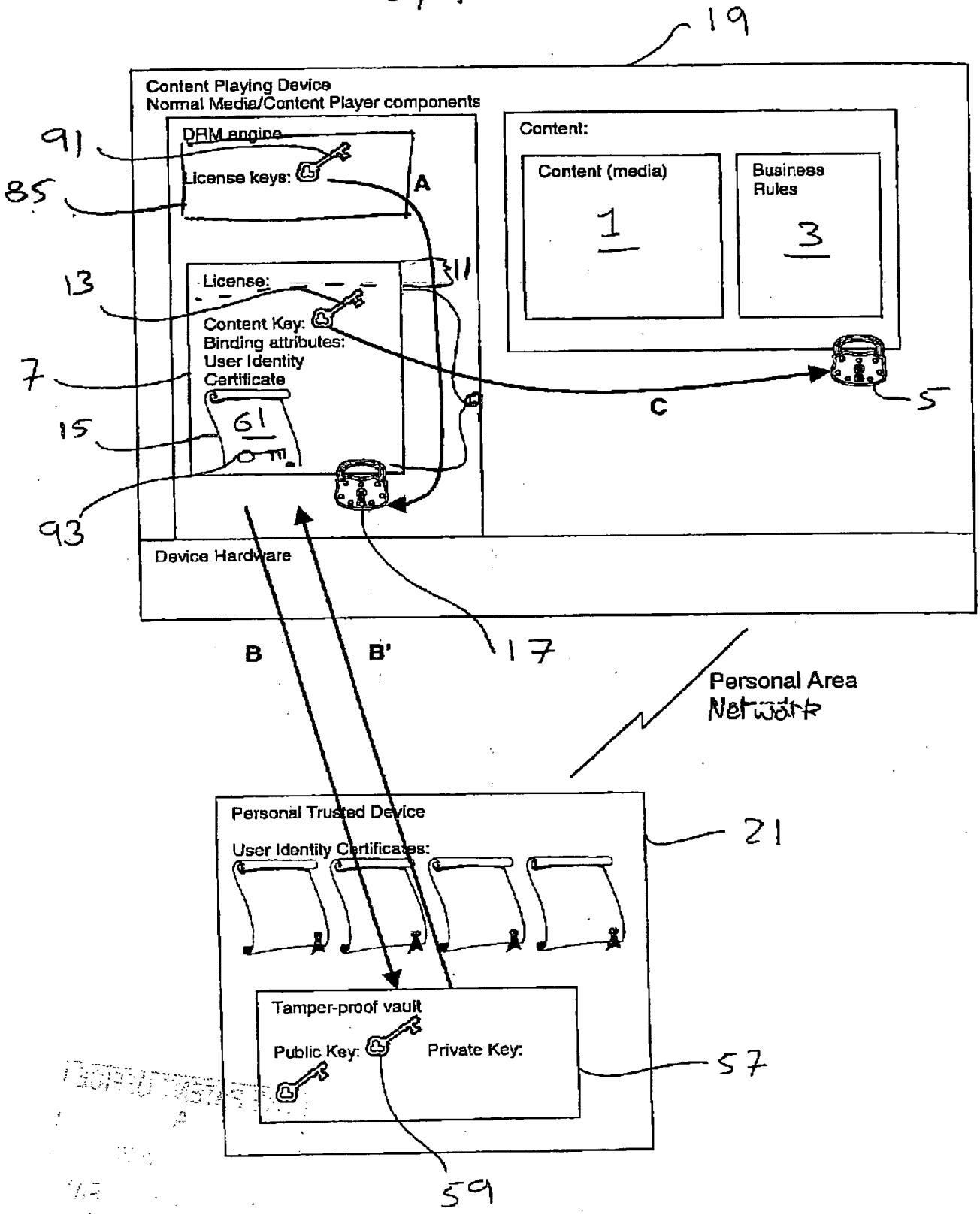

517
19
Content Playing Device
Normal Media/Content Player components
DRM engine
License keys:
91
85
A
License:
311
13
Content Key:
Binding attributes:
User Identity
Certificate
7
61
15
93
Content:
Content (media)
1
Business Rules
3
C
5
Device Hardware
B
B'
17
Personal Area Network
Personal Trusted Device
User Identity Certificates:
21
Tamper-proof vault
Public Key:
Private Key:
57
59

Figure 7

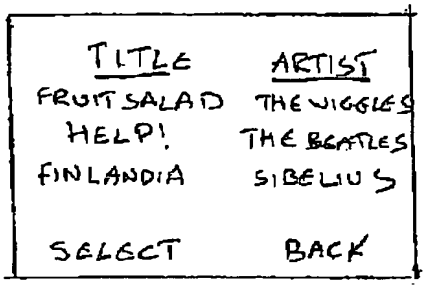


Figure 8a

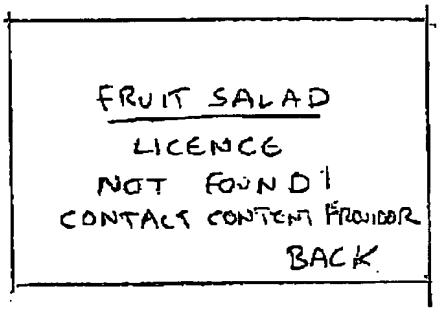


Figure 8b

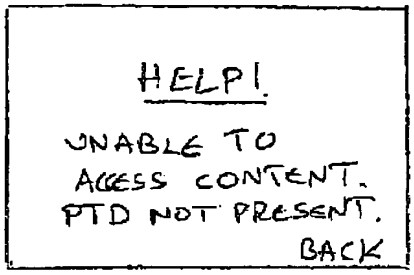


Figure 8c

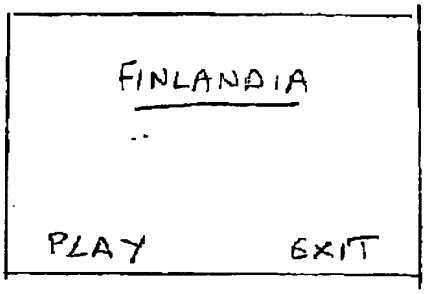


Figure 8d

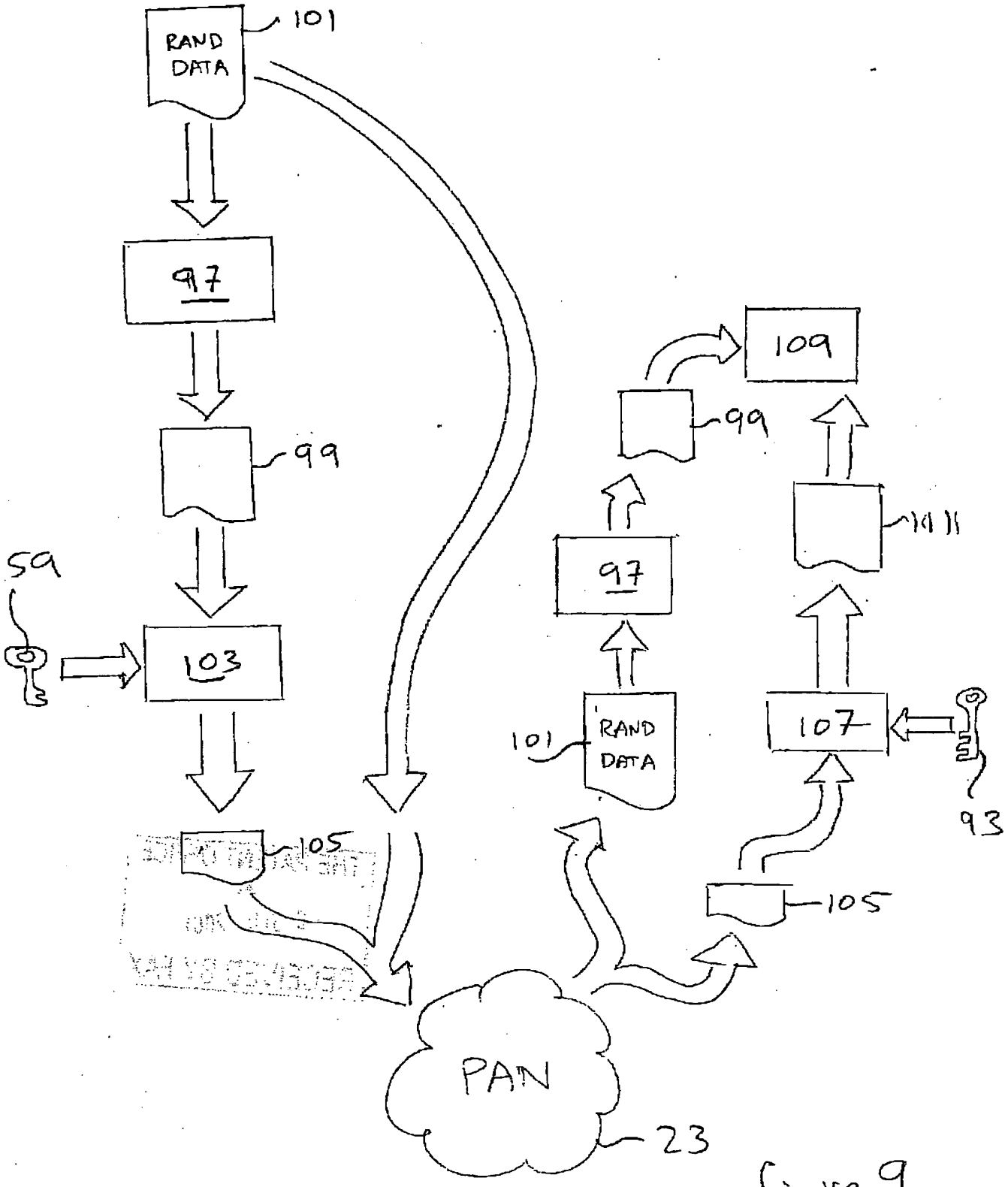

RAND DATA
101
97
99
59
103
105
109
99
97
111
101
RAND DATA
107
93
105
PAN
23

Figure 9

Leon, HURST et al
USSN 10/029,349 f. 12/28/01

This Page Blank (uspto)